(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 750 554**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **96 08053**

(51) Int Cl[6] : **H 04 L 9/32**, H 04 N 7/16

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 28.06.96.

(30) **Priorité :**

(43) **Date de la mise à disposition du public de la demande :** 02.01.98 Bulletin 98/01.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *THOMSON MULTIMEDIA SOCIETE ANONYME* — FR.

(72) **Inventeur(s) :** CAMPINOS ARNALDO et FISCHER JEAN BERNARD.

(73) **Titulaire(s) :** .

(74) **Mandataire :** THOMSON MULTIMEDIA.

(54) SYSTEME A ACCES CONDITIONNEL ET CARTE A PUCE PERMETTANT UN TEL ACCES.

(57) L'invention concerne un système à accès conditionnel permettant à un prestataire de services de ne fournir ses services qu'aux seuls utilisateurs ayant acquis des droits sur ces services.

Les services fournis par un prestataire de services sont constitués d'une information embrouillée par des mots de contrôle. Afin de garder secrets les mots de contrôle, ceux-ci sont fournis après avoir été encryptés avec un algorithme de clé K.

Les droits de chaque utilisateur sont envoyés dans des messages communément notés EMM (l'abréviation EMM étant issue de l'anglais "Entitlement Management Messages").

Selon l'invention, la clé K de l'algorithme d'encryptage des mots de contrôle est contenue dans les EMM.

FR 2 750 554 - A1

SYSTEME A ACCES CONDITIONNEL ET CARTE A PUCE PERMETTANT UN TEL ACCES

La présente invention concerne un système à accès conditionnel.

Un système à accès conditionnel permet à un prestataire de services de ne fournir ses services qu'aux seuls utilisateurs ayant acquis des droits sur ces services . C'est le cas , par exemple , des systèmes de télévision à péage .

Comme cela est connu de l'homme de l'art, le service fourni par un prestataire de services est constitué d'une information embrouillée par des mots de contrôle . L'information embrouillée ne peut être désembrouillée , et donc lue par l'utilisateur , qu'à hauteur des droits attribués à cet utilisateur . L'information embrouillée sera par la suite notée IE(ECG) , où ECG représente l'information non embrouillée (l'abréviation ECG est issue de l'anglais " Electronically Coded Good ") .

Afin de désembrouiller l'information , le prestataire de services fournit à chaque utilisateur les mots de contrôle qui ont servi à embrouiller l'information . De façon à garder secrets les mots de contrôle , ceux - ci sont fournis après avoir été chiffrés avec un algorithme de clé K . Les différents mots de contrôle chiffrés sont envoyés aux différents utilisateurs dans des messages communément notés ECM (l'abréviation ECM est issue de l'anglais " Entitlement Control Messages ") .

Afin de ne donner l'accès à son service qu'aux seuls utilisateurs autorisés, le prestataire de services fournit à chacun des utilisateurs une carte à puce et un décodeur .

La carte à puce permet , d'une part , de valider et d'enregistrer les droits qu'a l'utilisateur sur le service délivré et , d'autre part , de déchiffrer , à l'aide de la clé K , les mots de contrôle chiffrés . A cette fin, la carte à puce contient donc la clé K de l'algorithme qui a permis le chiffrement des mots de contrôle .

Le décodeur , quant à lui , permet de désembrouiller l'information embrouillée à partir de l'information constituée par les mots de contrôle déchiffrés issus de la carte à puce .

Les droits de chaque utilisateur sont envoyés dans des messages communément notés EMM (l'abréviation EMM étant issue de l'anglais "Entitlement Management Messages") .

Selon l'art connu, l'EMM dédié à un utilisateur contient trois informations principales :

- une première information donnant l'adresse de la carte de l'utilisateur ;

- une deuxième information donnant la description des droits de l'utilisateur ;

- une troisième information permettant de valider l'EMM et de vérifier que les droits de l'utilisateur contenus dans l'EMM sont bien les droits réservés à l'utilisateur.

Lorsque le décodeur d' un utilisateur reconnait l' adresse de la carte qui lui est associée parmi les différentes adresses distribuées par le prestataire de services , l'EMM correspondant à l'adresse reconnue est analysé. L'analyse de l'EMM est effectuée à l'aide d'un algorithme d'analyse dépendant de la clé K de chiffrement des mots de contrôle .

La clé K de l'algorithme de chiffrement des mots de contrôle est contenue dans chaque carte - utilisateur . Il s'ensuit que le piratage d'une seule carte peut conduire à la connaissance de la clé K. Des droits d'utilisation illicites peuvent alors être créés et enregistrés sur toutes les autres cartes fournies par le prestataire de services et contenant la même clé K. Il est aussi possible de recopier sur ces autres cartes les droits de l'utilisateur contenus dans la carte piratée. Le service fourni par le prestataire n'est alors plus protégé.

Afin de pallier ces inconvénients, il est connu que le prestataire de services modifie, à intervalles de temps réguliers, la clé de l'algorithme de chiffrement des mots de contrôle . Le prestataire de services doit alors fournir à chaque utilisateur une nouvelle carte contenant une nouvelle clé K.

Ceci représente un inconvénient , notamment en terme de coûts , puisque le nombre de cartes - utilisateur est souvent très élevé. Ce nombre peut en effet atteindre fréquemment plusieurs centaines de milliers , voire plusieurs millions .

L'invention ne présente pas cet inconvénient.

La présente invention concerne un nouveau système à accès conditionnel . Plus particulièrement , l'invention concerne une nouvelle définition des EMM ainsi qu'une nouvelle définition des différentes fonctions contenues dans la carte - utilisateur .

Ainsi , l'invention concerne - t - elle un message (EMM) permettant de définir les droits que possède un utilisateur sur un service constitué d'une information embrouillée à l'aide de mots de contrôle, les mots de contrôle étant fournis à l'utilisateur après avoir été chiffrés par un algorithme de clé K, le message (EMM) contenant une information permettant de le valider et de vérifier que les droits qu'il contient sont les droits réservés à l'utilisateur . Le message (EMM) contient la clé K de l'algorithme de chiffrement des mots de contrôle .

L'invention concerne également un procédé permettant de désembrouiller un service embrouillé fourni à au moins un utilisateur ,ledit service étant embrouillé à l'aide de mots de contrôle , ledit procédé comprenant une étape permettant de fournir à l'utilisateur un premier message (ECM) contenant au moins un mot de contrôle chiffré avec un algorithme de clé K, une étape permettant de fournir à l'utilisateur un second message (EMM) contenant les droits de l'utilisateur et une étape permettant de valider et de vérifier que les droits contenus dans le second message (EMM) sont les droits réservés à l'utilisateur . La clé K est distribuée à l'utilisateur dans le second message (EMM) .

L'invention concerne aussi une carte à puce permettant de déchiffrer les mots de contrôle chiffrés qu'elle reçoit, les mots de contrôle étant chiffrés par un algorithme de clé K, et permettant , après déchiffrement , de désembrouiller un service embrouillé , la carte comprenant un circuit de validation des droits de l'utilisateur contenant une première clé de contrôle permettant de contrôler la validation des droits de l' utilisateur et un circuit de validation des conditions d'accès associées au service , le circuit de validation des conditions d'accès contenant une seconde clé de contrôle .La première clé de contrôle est différente de la clé K .Selon le mode de réalisation préférentiel de l'invention la première clé de contrôle est une clé propre à la carte et donc différente d'une carte à l'autre .

L'invention concerne encore un système à accès conditionnel permettant à un prestataire de services de ne fournir ses services qu'aux

utilisateurs ayant acquis des droits sur ces services , lesdits services étant constitués d'une information embrouillée par des mots de contrôle , ledit système comprenant , pour chaque utilisateur , au moins un décodeur et au moins une carte - utilisateur , ladite carte contenant , d'une part , des circuits permettant de valider et d'enregistrer les droits de l'utilisateur sur le service délivré par le prestataire , lesdits droits étant véhiculés jusqu'à la carte - utilisateur par un premier message (EMM) et , d'autre part , des circuits permettant de restituer les mots de contrôle à partir des mots de contrôle chiffrés par un algorithme de clé K , lesdits mots de contrôle chiffrés étant véhiculés jusqu'à la carte - utilisateur par un second message (ECM) . La carte - utilisateur est une carte telle que celle selon l'invention mentionnée ci - dessus et le premier message (EMM) est un message permettant de définir les droits que possède l'utilisateur tel que celui selon l'invention mentionné ci - dessus .

Un avantage de l'invention est de renforcer considérablement la protection des services fournis par le prestataire . Le piratage d'une ou de plusieurs cartes - utilisateur n'offre alors pratiquement plus aucun intérêt pour le pirate éventuel .

D'autres caractéristiques et avantages de l'invention apparaitront à la lecture d'un mode de réalisation préférentiel fait avec référence aux figures ci-annexées parmi lesquelles :

- les figures 1a et 1b représentent respectivement un premier et un deuxième format d' EMM selon l'art antérieur ;
- la figure 2 représente le format d'un ECM selon l'art antérieur;
- la figure 3 représente le synoptique d'une carte - utilisateur selon l'art antérieur ;
- les figures 4a et 4b représentent respectivement un premier format et un deuxième format d'EMM selon l'invention;
- la figure 5 représente le synoptique d'une carte - utilisateur selon l'invention .

Sur toutes les figures, les mêmes repères désignent les mêmes éléments.

La figure 1a représente un premier format d' EMM selon l'art antérieur.

L'EMM représenté en figure 1a est composé d'un corps C1a contenant les trois informations principales mentionnées précédemment,

et d'un en-tête 4, communément appelée "Header" , et dont le contenu (H1) donne , entre autre , le type et la taille des informations contenues dans le corps C1a.

Le corps C1a est constitué d'une première information 1 contenant l'adresse (AD) de la carte de l'utilisateur, d'une deuxième information 2 contenant une description des droits de l'utilisateur, et d'une troisième information 3 contenant une donnée $HASH_K$. La donnée $HASH_K$ est une grandeur qui dépend de la clé K et qui permet d'effectuer l'analyse de l'EMM mentionnée précédemment .

La figure 1b représente un deuxième format d' EMM selon l'art antérieur.

L'EMM est constitué d'un en-tête 4 , et d'un corps C1b .

Le corps C1b est constitué des informations 5 et 6 contenant respectivement l'adresse AD de la carte - utilisateur et la description des droits de l'utilisateur chiffrés avec l'algorithme de clé K et relatifs à l'adresse AD ($E(\text{droits de l'utilisateur})_{K,AD}$). Selon ce format d'EMM , la validation et la vérification des droits contenus dans l'EMM sont effectués par l'opération de déchiffrement des droits chiffrés .

La figure 2 représente le format d'un ECM selon l'art antérieur .

L'ECM est constitué d'un corps C2 et d'un en-tête 7 dont le contenu (H2) donne , entre autre , le type et la taille des informations contenues dans le corps C2 .

Le corps C2 comprend ,entre autre, une première information 8 contenant l'ensemble des conditions d'accès associées au service fourni par le prestataire de services , une deuxième information 9 contenant un mot de contrôle Cwi chiffré avec l'algorithme de clé K ($E(CWi)_K$) et une troisième information 10 contenant une donnée $HASH_K$ dépendant de la clé K et permettant de valider et de vérifier le contenu des conditions d'accès .Le mot de contrôle Cwi représente le mot de contrôle courant , c'est - à - dire le mot de contrôle permettant de désembrouiller la partie du programme en cours de lecture.

Comme cela est connu de l'homme de l'art,généralement, l'ECM qui contient Cwi contient aussi un deuxième mot de contrôle . Ce deuxième mot de contrôle est le mot de contrôle de la période de

désembrouillage suivante , c'est - à - dire le mot de contrôle courant de l'ECM qui doit succéder à l'ECM qui contient Cwi comme mot de contrôle courant .Ce deuxième mot de contrôle n'a pas été représenté sur la figure 2 afin de ne pas alourdir inutilement le dessin .

Comme cela est connu de l'homme de l'art , les ECM sont envoyés par le prestataire de services avec l'information embrouillée IE(ECG) .

Le format d'ECM décrit en figure 2 n'est qu'un exemple de format d'ECM. En particulier , l'ordre des différents blocs (7 , 8 , 9 ,10) constituant l'ECM décrit en figure 2 peut être modifié .

La figure 3 représente le synoptique d'une carte - utilisateur selon l'art antérieur .

La carte-utilisateur 11 contient cinq circuits principaux :

- un circuit 12 de validation des droits de l'utilisateur ;
- un circuit 13 de mémorisation des droits validés de l'utilisateur
- un circuit 14 de contrôle d'accès ;
- un circuit 15 de validation des ECM ;
- un circuit 27 de déchiffrement des mots de contrôle chiffrés.

Quel que soit le format de l'EMM (cf. figures 1a et 1b), le circuit de validation 12 permet d'effectuer sur les EMM les opérations mentionnées précédemment de reconnaissance d'adresse de l'utilisateur et d'analyse des droits de l'utilisateur . A cette fin, le circuit de validation 12 contient la clé K de l'algorithme de chiffrement . Si l'EMM est validé , les droits de l'utilisateur contenus dans l'EMM sont mémorisés dans le circuit 13 de mémorisation des droits validés .

Le circuit de validation 15 des ECM permet d'effectuer sur les conditions d'accès 8 contenues dans les ECM des opérations identiques à celles effectuées par le circuit de validation 12 sur les droits de l'utilisateur. Le circuit de validation 15 contient la clé K .

Le circuit de déchiffrement 27 permet de déchiffrer les mots de contrôle . A cette fin, le circuit de déchiffrement 27 contient aussi la clé K de l'algorithme de chiffrement des mots de contrôle.

Le circuit de contrôle d'accès 14 compare les conditions d'accès validées aux droits validés de l'utilisateur . Si les conditions

d'accès validées correspondent aux droits validés de l'utilisateur , un signal S , issu du circuit de contrôle d'accès 14 et appliqué au circuit de déchiffrement 27 , autorise le déchiffrement des mots de contrôle chiffrés E (Cwi)$_K$ provenant du circuit de validation15 .Dans le cas contraire , le signal S n'autorise pas le déchiffrement.

A l'issue des différentes étapes du processus de déchiffrement, les mots de contrôle déchiffrés Cwi sont générés par le circuit de déchiffrement 27 de façon à permettre le désembrouillage de l'information embrouillée IE(ECG).

Comme cela a été mentionné précédemment , le piratage d'une seule carte - utilisateur , en permettant l'accès à la clé K , conduit à détruire la protection de l'ensemble des services fournis par le prestataire.

La figure 4a représente un premier format d'EMM selon l'invention.

Le corps C3a de l'EMM de l'utilisateur est ici composé de quatre informations principales :

- les informations 1 et 2 constituant respectivement l'adresse de l'utilisateur et la description des droits de l'utilisateur ;
- une information 16 contenant la clé K de l'algorithme de chiffrement des mots de contrôle ;
- une information 17 contenant une donnée de hachage $HASH_{KC}$, où KC est une clé différente de la clé K . Selon le mode de réalisation préférentiel de l'invention, la clé KC est propre à chaque utilisateur et donc différente d'une carte à l'autre . Selon d'autres modes de réalisation , la clé KC est propre à un groupe de cartes - utilisateur .

La figure 4b représente un deuxième format d'EMM selon l'invention.

Le corps C3b de l'EMM comprend trois informations principales:

- les informations 18 et 19 constituant respectivement l'adresse AD de la carte - utilisateur et la description des droits de l'utilisateur encryptés avec l'algorithme de clé KC et relatifs à l'adresse AD (E(droits de l'utilisateur)$_{KC,AD}$) . La clé KC est différente de la clé K . Selon le mode de réalisation préférentiel de l'invention , la clé KC est propre à chaque

carte - utilisateur et donc différente d'une carte à l'autre . Selon d'autres modes de réalisation la clé KC est propre à un groupe de cartes - utilisateur .

Selon ce format d'EMM , la validation et la vérification des droits contenus dans l'EMM sont effectués par l'opération de déchiffrement des droits chiffrés .

- une information 20 contenant la clé K de chiffrement des mots de contrôle chiffrés avec l'algorithme de clé KC ($E(K)_{KC}$) .

Avantageusement , quel que soit le format de l'EMM , la clé K de chiffrement des mots de contrôle n'est pas contenue dans la carte de l'utilisateur tant que les EMM n' ont pas été transmis à l'utilisateur .

La figure 5 représente le synoptique d'une carte-utilisateur selon l'invention ainsi que les ECM et les EMM selon l'invention.

La carte-utilisateur 21 contient cinq circuits principaux :

- un circuit 22 de validation des droits de l'utilisateur ;
- un circuit 23 de mémorisation des droits validés de l'utilisateur;
- un circuit 24 de contrôle d'accès ;
- un circuit 25 de validation des ECM ;
- un circuit 26 de déchiffrement des mots de contrôle chiffrés.

L'EMM de la figure 5 est du type représenté en figure 4a . La carte - utilisateur selon l'invention peut cependant fonctionner avec des EMM tels que ceux représentés en figure 4b .

Selon l'invention, les EMM sont analysés à l'aide d'un algorithme de validation contrôlé par la clé KC . La clé KC est contenue dans le circuit de validation 22 .

Les ECM sont , quant à eux , analysés à l'aide d'un algorithme de validation contrôlé par une clé KSP .A cette fin , dans le cadre de l'invention, les ECM contiennent une information 28 contenant une donnée $HASH_{KSP}$ dépendant de la clé KSP . La clé KSP est contenue dans le circuit de validation 25 . La clé KSP est différente de la clé K . Selon le mode de réalisation préférentiel de l'invention , la clé KSP est propre au prestataire de services .

Le circuit de contrôle d'accès 24 compare les conditions d'accès validées aux droits validés de l'utilisateur .

Si les conditions d'accès validées correspondent aux droits validés de l'utilisateur , un signal Y(K) issu du circuit de contrôle d'accès 24 et appliqué au circuit de déchiffrement 26 autorise le déchiffrement des mots de contrôle . Le signal Y(K) contient la clé K de façon à transmettre celle - ci au circuit de déchiffrement 26 .Les mots de contrôle chiffrés $E(Cwi)_K$ sont envoyés du circuit de validation 25 vers le circuit de déchiffrement 26 . Le déchiffrement des mots de contrôle est alors effectué .A l'issue des différentes étapes du processus de déchiffrement , les mots de contrôle déchiffrés Cwi sont générés par le circuit de déchiffrement 26 de façon à permettre le désembrouillage de l'information embrouillée .

Si les conditions d'accès validées ne correspondent pas aux droits validés de l'utilisateur , le déchiffrement des mots de contrôle n'est pas autorisé .

Selon l'invention , la validation des droits d'un utilisateur est contrôlée par une clé KC propre à l'utilisateur ou à un groupe d'utilisateurs . Il s'ensuit que le piratage d'une carte - utilisateur ne peut conduire qu' à mettre en cause la carte piratée elle-même ainsi que les cartes - utilisateur du même groupe d'utilisateurs si la clé KC est partagée par un même groupe d'utilisateurs .

Avantageusement , toutes les autres cartes - utilisateur demeurent protégées .

Selon le mode de réalisation de l'invention décrit ci - dessus , la clé K est la même pour tous les services fournis par le prestataire. L'invention permet la mise en oeuvre de modes de réalisation pour lesquels les différents services fournis par le prestataire sont embrouillés avec des mots de contrôle chiffrés avec un algorithme dont la clé de chiffrement diffère d'un service à l'autre ou d'un groupe de services à l'autre .

Ceci est particulièrement avantageux dans le cas des systèmes communément appelés systèmes "off-line" pour lesquels l'information embrouillée IE(ECG) et les ECM sont contenus sur des supports autonomes d'informations tels que, par exemple, des CD (de l'anglais

"Compact Disc"), des DVD (de l'anglais ("Digital Video Disc") ou encore des CD-ROM (de l'anglais "Compact-Disc Read Only Memory").

Avantageusement , le piratage d'une carte - utilisateur se trouve alors encore plus dépourvu d'intérêt que dans le cas où tous les services du prestataire sont embrouillés avec des mots de contrôle chiffrés avec la même clé K . En effet , le piratage d'une carte - utilisateur ne conduit alors qu'a un accès très partiel des différents services fournis par le prestataire .

Le fait d'embrouiller différents services , tels que par exemple des films , avec un algorithme dont les clés diffèrent d'un service à l'autre n'est pas envisageable dans le cadre des systèmes à accès conditionnel de l'art antérieur pour lesquels la clé de l'algorithme de chiffrement des mots de contrôle d'un service et la clé associée à l'algorithme de validation des droits de l'utilisateur sont identiques .

En effet, il faudrait alors que le prestataire de services fournisse à chaque utilisateur une carte propre à chaque service ou groupe de services. Une telle multiplication des cartes n'est pas réaliste , aussi bien pour des raisons d'ordre pratique que pour des raisons de coûts.

De façon générale , quelque soit le mode de réalisation de l'invention , c'est - à - dire que les différents services fournis par le prestataire soient associés à une clé de chiffrement des mots de contrôle K unique ou à différentes clés de chiffrement Kj (j = 1 , 2 , ... , m) , l'invention concerne aussi bien les systèmes à accès conditionnel de type "off - line" que les systèmes à accès conditionnel de type "on-line" pour lesquels l'information embrouillée IE(ECG) est une information constituée d'un signal distribué simultanément aux différents clients du prestataire de services à partir d'une source unique .

REVENDICATIONS

1. Message (EMM) permettant de définir les droits (2) que possède un utilisateur sur un service constitué d'une information (IE (ECG)) embrouillée à l'aide de mots de contrôle (Cwi), lesdits mots de contrôle étant fournis à l'utilisateur après avoir été chiffrés par un algorithme de clé K, ledit message (EMM) contenant une information permettant de le valider et de vérifier que les droits qu'il contient sont les droits réservés à l'utilisateur, ladite information permettant de valider le message et de vérifier les droits qu'il contient étant contrôlée par une clé (KC), caractérisé en ce qu'il contient la clé K de l'algorithme de chiffrement des mots de contrôle .

2. Message (EMM) selon la revendication 1 , caractérisé en ce que la clé (KC) contrôlant l'information permettant de le valider et de vérifier les droits qu'il contient est différente de la clé K de l'algorithme de chiffrement des mots de contrôle.

3. Message (EMM) selon la revendication 1 ou 2 , caractérisé en ce que la clé (KC) contrôlant l'information permettant de le valider et de vérifier les droits qu'il contient est propre à chaque utilisateur ou groupe d'utilisateurs.

4. Procédé permettant de désembrouiller un service embrouillé (IE(ECG)) fourni à au moins un utilisateur, ledit service étant embrouillé à l'aide de mots de contrôle (Cwi) , ledit procédé comprenant une étape permettant de fournir à l'utilisateur un premier message (ECM) contenant au moins un mot de contrôle chiffré avec un algorithme de clé K , une étape permettant de fournir un second message (EMM) contenant les droits de l'utilisateur et une étape permettant de valider et de vérifier que les droits contenus dans le second message (EMM) sont les droits réservés à l'utilisateur , caractérisé en ce que la clé K est distribuée à l'utilisateur dans le second message (EMM).

5. Procédé selon la revendication 4 , caractérisé en ce que l'étape permettant de valider et de vérifier les droits contenus dans le second message (EMM) est effectuée à l'aide d'une information contrôlée par une clé (KC) différente de la clé K.

6. Procédé selon la revendication 5 , caractérisé en ce que la clé (KC) utilisée pour contrôler l'information est propre à chaque utilisateur ou à un groupe d'utilisateurs.

7. Carte à puce (21) permettant de déchiffrer les mots de contrôle chiffrés ($E(Cwi)_K$) qu'elle reçoit, lesdits mots de contrôle étant chiffrés par un algorithme de clé K , et permettant, après déchiffrement, de désembrouiller un service embrouillé fourni à un utilisateur , ladite carte comprenant un circuit (22) de validation des droits de l'utilisateur contenant une première clé de contrôle (KC) permettant de contrôler la validation des droits de l'utilisateur et un circuit (25) de validation des conditions d'accès associées au service fourni par le prestataire de services, ledit circuit (25) de validation des conditions d'accès contenant une seconde clé de contrôle (KSP) , caractérisée en ce que la première clé de contrôle (KC) est différente de la clé K.

8. Carte (21) selon la revendication 7, caractérisée en ce que la première clé de contrôle (KC) est une clé propre à ladite carte ou à un groupe de cartes .

9. Carte selon la revendication 7 ou 8 , caractérisée en ce que la seconde clé de contrôle (KSP) est une clé propre au prestataire de services .

10. Système à accès conditionnel permettant à un prestataire de services de ne fournir ses services qu'aux utilisateurs ayant acquis des droits sur ces services , lesdits services étant constitués d'une information embrouillée (IE(ECG)) par des mots de contrôle (Cwi), ledit système comprenant , par utilisateur , au moins un décodeur et au moins une carte-utilisateur (21), ladite carte contenant , d'une part , des circuits (22 ,23) permettant de valider et d'enregistrer les droits de l'utilisateur sur le

service délivré par le prestataire , lesdits droits étant véhiculés jusqu'à la carte - utilisateur par un premier message (EMM) et , d'autre part , des circuits (26) permettant de restituer les mots de contrôle (Cwi) à partir des mots de contrôle encryptés ($E(Cwi)_K$) par un algorithme de clé K , lesdits mots de contrôle encryptés étant véhiculés par un second message (ECM) , caractérisé en ce que la carte-utilisateur (21) est une carte selon l'une quelconque des revendications 7 à 9 et en ce que le premier message (EMM) est un message selon l'une quelconque des revendications 1 à 3 .

11. Système selon la revendication 10, caractérisé en ce qu'il est du type " on - line ".

12. Système selon la revendication 10 , caractérisé en ce qu'il est du type " off - line " .

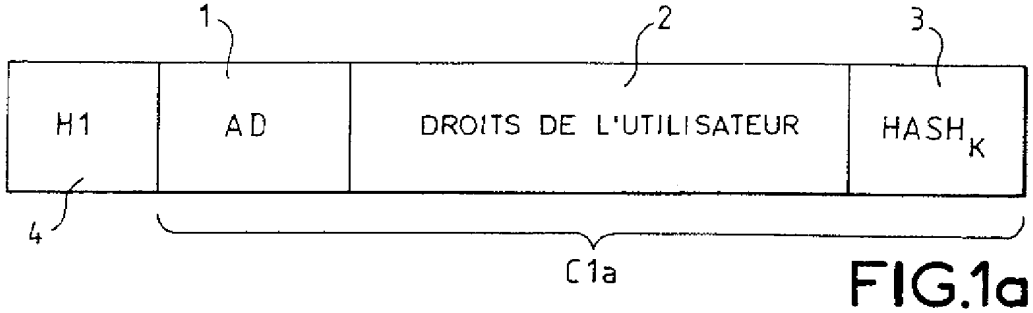

FIG.1a

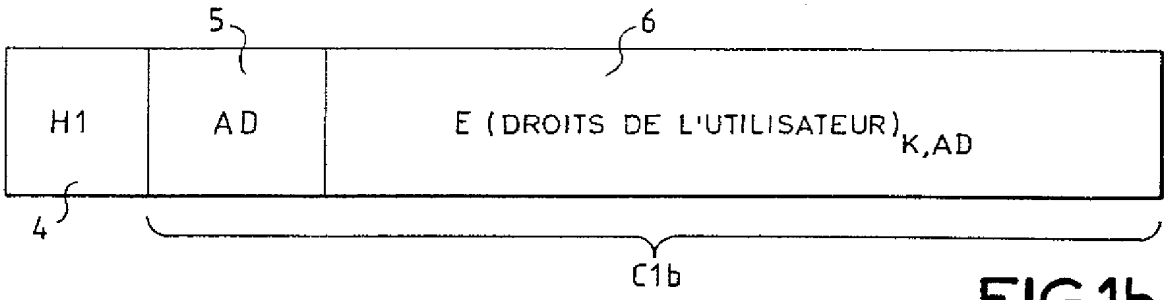

FIG.1b

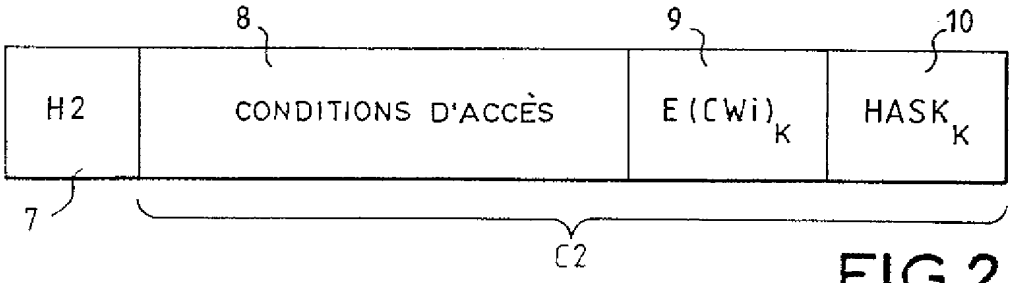

FIG.2

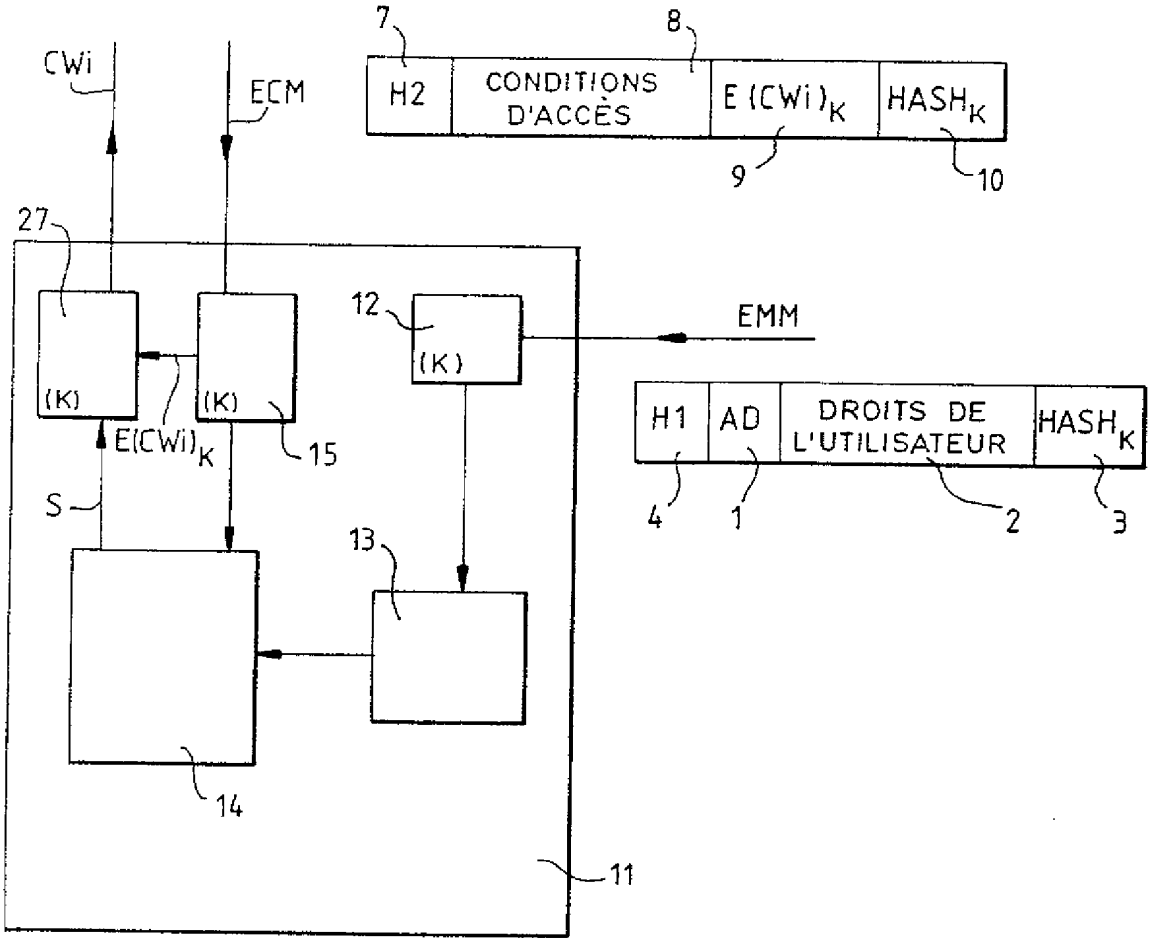

FIG.3

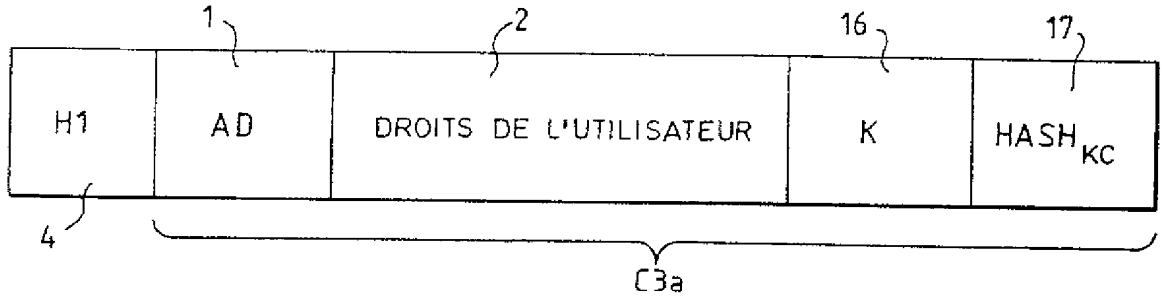

FIG.4a

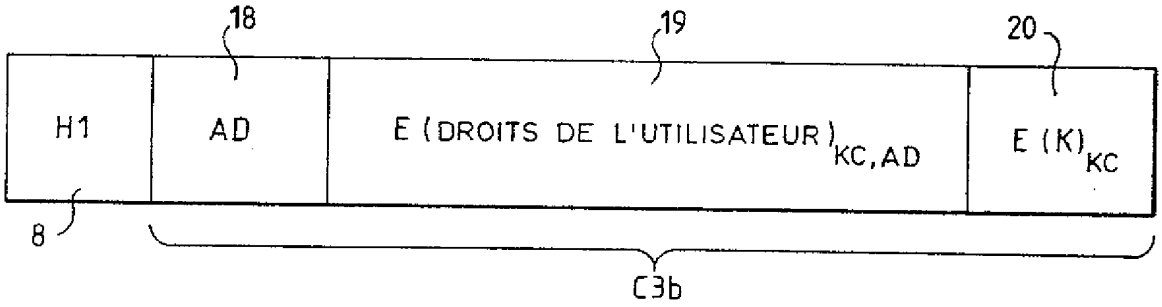

FIG.4b

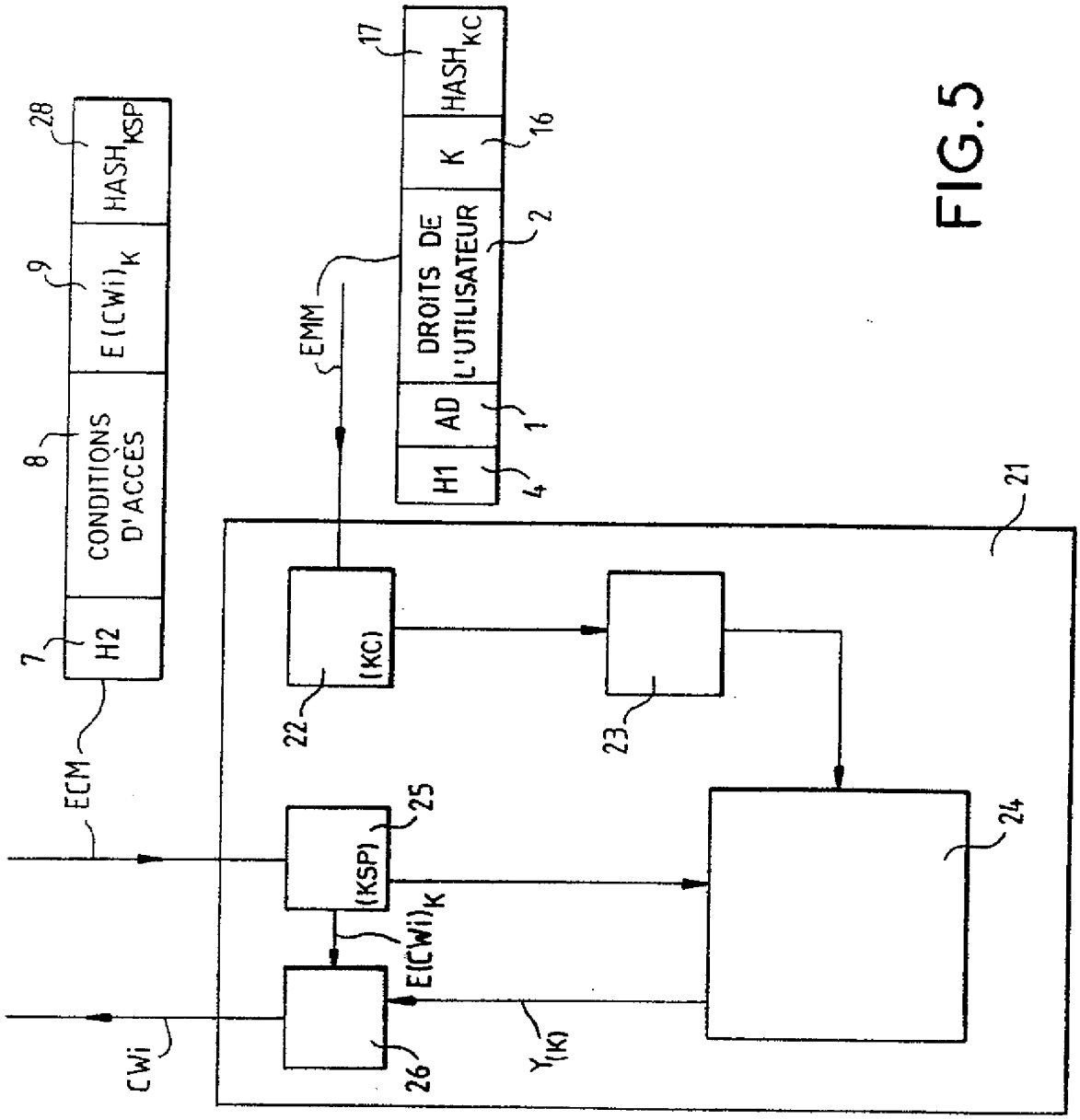

FIG.5

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2750554
N° d'enregistrement national

FA 529788
FR 9608053

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée	
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	EP 0 506 435 A (SCIENTIFIC ATLANTA) 30 Septembre 1992 * page 8, ligne 41 - page 13, ligne 13 * * figures 7-10 *	1-12	
A	EP 0 461 029 A (MATRA COMMUNICATION ;FRANCE TELECOM (FR); TELEDIFFUSION FSE (FR)) 11 Décembre 1991 * page 4, colonne 4, ligne 24 - page 6, colonne 8, ligne 4 * * figures 2,3 *	1-5,10	
A	EP 0 375 539 A (EUROP RECH ELECTR LAB) 27 Juin 1990 * page 3, colonne 4, ligne 5 - page 4, colonne 6, ligne 38 * * page 5, colonne 7, ligne 31 - colonne 8, ligne 11 * * figures 1-5 *	7-12	
A	WO 95 28058 A (FRANCE TELECOM ;TELEDIFFUSION FSE (FR)) 19 Octobre 1995 * page 4, ligne 9 - page 5, ligne 28 * * page 11, ligne 4 - page 15, ligne 34 * * figures 4-9 *	1-6	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6) H04N

Date d'achèvement de la recherche	Examinateur
10 Mars 1997	Van der Zaal, R

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

1

EPO FORM 1503 03.82 (P04C13)